Kivédhető az adatszivárgás?

Az adatszivárgás ténye nem új keletű, máig sok gondot okoz a megelőzése. Üzleti érdek védeni az érzékeny adatokat. Mennyire múlik emberi tényezőn, kivédhető-e technológiai lefedettséggel, esetleg a hr felelőssége a megelőzés?

Oktatással

FORRÁS: MAGICOM

Gasparetz András ügyvezető igazgató, MagiCom

Szükséges a megfelelő szabályozórendszer

Az adatszivárgás ellen az információvédelem teljes eszköztárát – fizikai, műszaki és adminisztratív kontrollok – felhasználják a szervezetek. Ezek fő célja az emberi figyelmetlenség, a tudatlanság és a szándékos károkozás kockázatának csökkentése. Az adatszivárgási incidensek forrása, okozója szinte mindig az ember, és így nem meglepő, hogy különböző statisztikák igen magas arányban, 70-80 százalékban emberi okokra vezetik vissza az adatszivárgásokat.

A hr szerepe, hogy már az alkalmazottak kiválasztásakor vegye figyelembe a szükséges és elsajátítandó ismeretanyagot és a személyi készségeket. Az emberek okozta kockázatok kezeléséhez elengedhetetlen a megfelelő szabályozórendszer. Ezen a kötelező és jogi hátteret adó elemen kívül kifejezetten fontosak a belépéskori és a rendszeres, ismétlő oktatások.

Lényeges, hogy valóban alakítsuk ki a helyes magatartásformák betartása iránti igényt. Ehhez erősen ajánlhatók az e-learninges megoldásokkal kombinált konzultációk. Ilyen módon jól mérhetővé válik a tényleges egyéni teljesítmény és a követendő szabályrendszer érthetősége is, azaz meghatározhatók azok a területek, amelyeknek az értelmezése gondot okoz a felhasználóknak.

Jó gyakorlatnak tekinthető a tudatosító programok végrehajtása, melyeknek részei lehetnek például a rendszeres hírlevelek, illetve a tanulsággal szolgáló nyilvános esettanulmányok. ■

Védelmi szoftverekkel

Az adatszivárgás csak másodsorban technológiai kérdés. Egy szervezetnél, ahol minősítik az adatokat és igazolható módon megteszik az ilyenkor elvárt biztonsági intézkedéseket, és ennek ellenére megtörténik az adatszivárgás, vagy igazolható a szándékosság, ez esetben a cselekmény büntethető is lehet. Ha valaki nagyon el akar vinni védett adatokat és professzionalista, akkor nagyon nehéz megakadályozni ebben. Sok esetben már csak a nyomait lehet regisztrálni. Ez pedig kimerítheti a titoksértés fogalmát.

Csupán néhány professzionális adatszivárgás elleni védelmi szoftver van a piacon. Általában a következő főbb funkciót látják el: egyrészt adatklasszifikációt támogatnak, megmondják, hogy melyek a védendő adatok, másrészt ezek a nagyon intelligens eseményvezérelt megoldások tartalom alapján támogatják azt az eljárásrendet, mely korlátozza a védendő adatokkal történő adatfeldolgozási és adatáramlási folyamatokat. Riportolják a felhasználói aktivitást, illetve monitorozzák a hálózati forgalmat. Ma szinte minden adatszivárgást kezelő megoldás rendelkezik végpontvédelmi modullal.

E megoldások kapcsán sok tízmilliós beruházásról beszélünk. Természetesen egy bank, egy mikro-, kis- vagy közepes vállalkozás esetében is mások a fenyegetettségek és a kockázatok, így a védelemre szánt költségkeretek sincsenek egy súlycsoportban. ■

FOTÓ: ITBUSINESS

Jakab Péter ügyvezető igazgató, MKB Bank, Bankbiztonság

Szofisztikált védelmi környezet kialakítása